

WHAT IS CLAIMED IS:

- 1 1. A method for communication of messages in a secure manner in a
2 communication environment which is subject to compromise, the method comprising:
3 providing an escrow agent, wherein said escrow agent generates a pair of keys
4 comprising a public key and a private key;
5 causing said escrow agent to communicate said public key to all parties within
6 a communication system to be used to support secure communication;
7 extracting at each party a common benchmark;
8 agreeing among each party on a starting interval key referenced to said
9 common benchmark;
10 causing each party to generate iteratively a next interval key independently of
11 each other party but with reference to an interval index, wherein said interval key is
12 encrypted by said public key; thereafter
13 initiating a secure communication between or among parties using reference to
14 said interval index and without communicating or exchanging their respective interval keys;
15 causing each party to a secure communication to encrypt a message to be
16 secured using the common interval key independently computed based on said common
17 interval index; and
18 causing said encrypted message to be communicated within said system such
19 that said encrypted message can be decrypted using said common interval key.
- 1 2. The method according to claim 1 wherein said parties exchange their
2 respective interval indexes and wherein the parties with the older interval indexes advance
3 their interval index and compute said interval key corresponding to the latest interval index.
- 1 3. The method according to claim 2 wherein each party destroys each
2 prior interval key after a new interval key is generated so that an older interval key cannot be
3 recovered.
- 1 4. The method according to claim 1 wherein said interval index is not
2 communicated to said escrow agent.
- 1 5. The method according to claim 1 wherein said starting interval key is
2 not communicated to said escrow agent.